



UNITED STATES MARINE CORPS

Marine Corps Recruit Depot/Western Recruiting Region
1600 Henderson Avenue Suite 235
San Diego, California 92140-5001

IN REPLY REFER TO:
DepO 5239.4B
5E

OCT 03 2001

DEPOT ORDER 5239.4B W/chl

From: Commanding General
To: Distribution List

Subj: APPROPRIATE USE OF GOVERNMENT INFORMATION TECHNOLOGY RESOURCES (GITR)

Ref: (a) IRM 5239-08 Computer Security Procedures (NOTAL)
(b) IRM 5239-10 Small Computer Systems Security (NOTAL)
(c) MARADMIN 162/00

1. Situation. The Marine Corps is in the midst of what is commonly called the information explosion. Central to the Marine Corps involvement in this is the rapid and continued growth of the Marine Corps Enterprise Network (MCEN). One of the empowering features of the MCEN is the ability to send and receive e-mail within the Marine Corps and the accessibility to send and receive outside the Marine Corps via the Internet. The Internet is another tool with virtually unlimited information resources and services that can widely disseminate information and can fulfill the Marine Corps information management needs and enhance connectivity in a "real time" manner. Even though all this information is available, we must all face the reality that our network infrastructure is limited in its capacity to funnel all of this information. Information resources like sending/receiving e-mail and accessing the World Wide Web (WWW) with its File Transfer Protocol (FTP) can seriously degrade network performance for other systems sharing the same network components. It is crucial that the Command's network remain responsive to mission critical needs. In order for this to occur, guidelines and Command policy must be in place for effective management of the limited resources. This Order provides guidance to all Marine Corps Recruit Depot (MCRD) and Western Recruiting Region (WRR) users and administrators using Government Information Technology Resources.

2. Cancellation. DepO 5239.4A

3. Mission. To establish procedures for the authorized use of Government Information Technology Resources (GITR). Resources addressed in this Order include, but are not limited to: Computer hardware and software, Telecommunications Infrastructure, Local Area Networks (LAN), Facsimile Machines, Electronic Mail (e-mail), and Internet Access. This Order is intended to compliment and underscore the guidance set forth in references (a) through (c).

4. Execution

a. Internet Connectivity. Connections to the Internet will only be established through official Marine Corps or Department of Defense (DoD) circuits. Access to the Internet via commercial service providers without an authorized waiver from the Designated Approving Authority (DAA), MCRD, San Diego, is not allowed. The DAA for MCRD, San Diego, is the Director, Communications and Information Systems Department (CISD), as appointed by the Commanding General.

b. Web Servers. The DAA will coordinate the web server access, and technical implementation for the Command. The establishment of WWW servers within this command must be approved with the DAA. Only Secure internal WWW

servers utilizing Secure Socket Layer (SSL) encryption will be advertised outside of the Marine Corps and then only with the approval and coordination of the DAA and Marine Corps Information Technology and Network Operation Center (MITNOC) Marine Corps Systems Command, Quantico, VA.

c. Internet Mail Services. The capability to send and receive e-mail to Internet addresses is available to all users having a valid network e-mail account. Commercial e-mail accounts (AOL, Hotmail, Earthlink, etc.) will not and can not be logged on from workstations connected to the MCEN. Too many users simultaneously sending and/or receiving large files potentially degrade network performance and deny access to others for Official use. A Simple Mail Transfer Protocol gateway is operational at MCRD, San Diego, to provide Internet e-mail access to the Depot.

d. Web Browsing and Data Transfers. The availability of Web browsers and FTP programs, coupled with the access to files available on Internet sites, and other open anonymous information servers pose the greatest potential for adverse impacts on network performance. Access to these resources must be controlled in order to provide a responsive network.

e. File Transfers. Downloading of large mission essential files should be limited to off-peak hours. Downloading during peak hours (i.e. 0730 - 1630) can adversely affect network performance. Further, the downloading of files with the extension .exe or .com will be directed to a "Download" folder on the Windows Desktop which will then be scanned using the DoD standard virus detection package prior to being executed (loaded).

f. Users. All computers, LAN, and Internet users employed by the government will be required to attend an annual Information Systems Security class approved by the DAA. All users will sign a Letter of Agreement acknowledging procedures for use of Government Computers, LAN, and Internet. Individuals will be held accountable for unauthorized or inappropriate use.

g. Personal Software/Hardware. No personally-owned hardware or software will be installed or used, without approval by the DAA. If approved, a "Personally-Owned Microcomputer Hardware/Software User Agreement" must be filled out and on file. Example of personally-owned includes, but is not limited to, computers, printers, scanners, programs, Personal Electronic Devices (i.e. personal digital devices, Palmtops, hand-held computers and wireless e-mail devices).

h. Government Laptops/Notebooks. Governments Laptops/Notebooks are used by personnel when traveling for the Command. There is a risk not only for loss of the Laptop/Notebook but also for the loss or modification of data and software stored on it. Even though the information may be unclassified, much of the information is sensitive and can cause potential damage to National Security if the information falls into the wrong hands. There have been many reported cases where laptop hardware has been tampered with and software modified. This includes documents and information that has been copied, printed and distributed to personnel that do not have the "Need to Know". Some basic guidelines must be followed when using a Laptop/Notebook.

(1) Laptops/Notebooks should never be left unattended. Keep it under your control at all times. If it is going through an x-ray system, keep an eye on it as much as possible, so that it is not out of sight.

OCT 19 1991

(2) Secure your Laptop/Notebook when in a Hotel/Billeting. One method is to place it out of sight in a locked suitcase. Avoid leaving your laptop unattended on a table at a conference.

(3) Do not store login names and/or passwords on the laptop. Disable the internal microphone and infrared interface fo equipped with either one or both.

(4) Configure the screen saver to require a password and set the time-out interval to a short period of time.

(5) Make sure the current approved Department of Defense Antivirus program is loaded and has the latest definition file loaded.

5. Administration and Logistics

a. Official and Personal Use. GITS are for Official Use and authorized purposes only. Use of these resources, to include access to the Internet, is authorized when work related and/or determined to be in the best interests of the Federal Government and the Marine Corps. Resources may also be used for brief incidental personal purposes, as long as all guidelines stated in this Order are met. Examples of using the resources are:

(1) Support DoD/DoN/USMC missions.

(2) Enhances the professional skills of Marine Corps personnel.

(3) Improve professional or personal skills as part of a formal academic education or military/civilian professional development program.

(4) For personal purposes, the use should be appropriate in frequency and duration.

b. Guidelines for Personal Use. Use of GITS is allowed under the following guidelines:

(1) Does not result in added costs to the Government.

(2) Does not adversely affect the performance of OFFICIAL DUTIES.

(3) Serves a legitimate public interest such as enhancing professional skills or improving morale.

(4) Is of minimal frequency and duration and occurs during an individual's personal time.

(5) Does not overburden government computing resources or communications systems.

(6) Is not used for purposes that adversely reflect upon the Marine Corps.

c. Prohibited Use. Use of GITS for purposes other than those described above is prohibited. Examples of prohibited use include, but are not limited to, the following:

(1) Illegal, fraudulent or malicious activities.

(2) Partisan political activity, political or religious lobbying or advocacy of activities on behalf of organizations having no affiliation with the Marine Corps or DoD.

(3) Activities whose purposes are for personal or commercial financial gain. These activities include solicitation of business services.

(4) Unauthorized fundraising.

(5) Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography or hate literature.

(6) Obtaining, installing, or using software in violation of the appropriate vendor's patent, copyright, trade mark, or license agreement.

(7) The creation, forwarding, or passing of chain letters.

d. Security. Storing, accessing, processing, or distributing classified, or otherwise sensitive (e.g. privacy act, proprietary, "FOR OFFICIAL USE ONLY", contractually or financially sensitive, etc.) information on a computer or network must be in accordance with applicable regulations.

e. Monitoring. The Information Systems Security Officer will periodically sample internet and e-mail traffic as directed by the DAA and report violations.

6. Command and Signal

a. Command

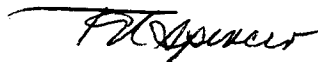
ch1
(1) Enforcement. Violations of the prohibited activities listed above may result in administrative or disciplinary action.

(2) Applicability. This Order is applicable to all personnel, both military and civilian at Marine Corps Recruit Depot, San Diego, and throughout the Western Recruiting Region.

b. Signal

(1) Summary of Revision. This Order has been completely revised and should be reviewed in its entirety.

(2) This Order is effective on date signed.


T. W. SPENCER
Chief of Staff

DISTRIBUTION: A



UNITED STATES MARINE CORPS
Marine Corps Recruit Depot/Western Recruiting Region
1600 Henderson Avenue Suite 238
San Diego, California 92140-5001

DepO 5239.4B Ch 1
1A
MAR 28 2003


DEPOT ORDER 5239.4B Ch 1

From: Commanding General
To: Distribution List

Subj: APPROPRIATE USE OF GOVERNMENT INFORMATION TECHNOLOGY RESOURCES
(GITR)

1. Situation. To direct a pen change to DepO 5239.4B, Appropriate use of Government Information Technology Resources (GITR).
2. Mission. To provide a change to the Depot Order.
3. Execution. Change paragraph 6a(1) to read as follows:

“(1) Enforcement. Violations of the prohibited activities listed **above** may result in administrative or disciplinary action.”
4. Administration and Logistics. Not applicable.
5. Command and Signal
 - a. Command. This Order is applicable to MCRD and WRR.
 - b. Signal. This Order is effective the date it is signed.


R. B. HUTCHINSON
By direction

DISTRIBUTION: A, G